:TED

Central Intelligence Agency
Washington, D.C. 20505

STAT

EA/ Executive Director

29 December 86

STAT

Note For: D/OS

Attention:

Subject: Draft National Security Decision Directive on Operations Security

[redacted]

Let me know by C.O.B. 6 January 87 if you have any comments.

EA/EXDIR

CC: C/CI staff

STAT

[redacted]

SENIOR INTERAGENCY GROUP (INTELLIGENCE)
WASHINGTON, D.C. 20505

ICS 86-3402
23 December 1986

MEMORANDUM FOR SENIOR INTERAGENCY GROUP - INTELLIGENCE

FROM: Executive Secretary

SUBJECT: Draft National Security Decision Directive on Operations Security

1. The attached above-cited document was prepared by the Intelligence Community in response to the President's Report to Congress on the Nation's Counterintelligence and Security Countermeasures Plans, Programs, and Capabilities. The Interagency Group/Countermeasures (Policy) concurred with the draft, and the Acting Chairman of the SIG-I, Acting Director of Central Intelligence Gates, approved it for your review.

2. There is no plan to hold a meeting of the SIG-I to discuss this draft document unless one of the members so requests. Please forward your comments or concurrence to the SIG-I Secretariat ( ) by 1200 hours on 7 January 1987. If the Secretariat has not heard from you by that time, or received a request for additional time for consideration, the Secretariat will take it that you concur with the draft as presented. STAT

3. Upon approval of the draft NSDD, it will be forwarded to the National Security Council.

STAT

Attachment:
Draft NSDD

DCI EXEC REG

UNCLASSIFIED

SUBJECT: Draft National Security Decision Directive on Operations Security

Distribution: (ICS 86-3402)

1 - Assistant to the President for
National Security Affairs
2 - Deputy Secretary of State
3 - Deputy Secretary of Defense
4 - Attorney General
5 - Chairman, Joint Chiefs of Staff
6 - Chairman, IG/CM(P)
7 - Chairman, IG/CM(T)
8 - Director, Federal Bureau of Investigation
9 - Director, National Security Agency
10 - Director, Intelligence Community Staff
11 - Executive Director, Central Intelligence Agency
12 - Deputy Assistant Secretary for Intelligence,
Department of Energy
13 - General Counsel, Department of Commerce
14 - Director, Office of Personnel Management
15 - Director, Information Security Oversight Office,
GSA
16 - Director, Office of Management and Budget

UNCLASSIFIED

DRAFT

National Security Decision
Directive Number _____

NATIONAL OPERATIONS SECURITY PROGRAM

BACKGROUND

Security programs and procedures already exist to protect classified matters. However, information generally available to the public as well as certain detectable activities exist that provide indications concerning classified or sensitive information or undertakings. Such indicators may be exploited by those seeking to neutralize or to take advantage of US Government actions that affect national security. Application of the Operations Security (OPSEC) process promotes operational effectiveness by guarding against the inadvertent compromise of sensitive or classified US Government activities, capabilities, or intentions.

OPERATIONS SECURITY

The operations security process involves five steps: identification of critical information, analysis of the threat, analysis of the vulnerabilities, assessment of the risks, and application of appropriate countermeasures. It begins with an examination of the totality of an activity to determine what exploitable, but essentially unclassified indicators could be acquired in light of the known collection capabilities of potential adversaries. Indicators usually evolve from openly available data and other detectable actions. Certain of these indicators may be pieced together or interpreted to discern

critical information. Indicators most often stem from the routine administrative, physical, or technical actions taken to prepare for, or execute a plan or activity. Once the incicators are identified, they are analyzed against the threat to determine the extent to which they could reveal critical information.

Commanders and managers then use these threat and vulnerability analyses in their risk assessment to assist in selecting and applying practical countermeasures to mitigate or nullify selected indicators. Indicators may be controlled or protected, as appropriate, using the full range of OPSEC measures.

OPSEC is, thus, a systematic and proved process by which the US Government and its supporting contractors can deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified indicators associated with the planning and execution of sensitive government activities.

APPLICATION

Indicators and vulnerabilities are best identified before activities start through detailed OPSEC planning. They may also be identified during or after the conduct of routine functional activities by analyzing how functions are actually performed and the procedures used. Planning and analysis proceed from the adversaries' perspectives. To assist in OPSEC planning and analysis, OPSEC planning guidance must be develcped jointly by those most familiar with

the operational aspects of a particular activity together with their supporting intelligence elements.

OPSEC planning guidance should consider those critical aspects of an activity which should be protected in light of US and adversary goals, estimated key adversary questions, probable adversary knowledge, desirable and harmful adversary appreciations, and pertinent intelligence threats, as well as an outline of projected OPSEC measures.

In the OPSEC process, it is important to distinguish between the threat and vulnerability analysis phases and the phase in which OPSEC measures are applied. Recommendations on the use of OPSEC measures are based on the joint operational-intelligence analyses, but ultimate decisions on their implementation are made by commanders, supervisors, or program managers who determine what aspects will be protected. The decisionmaker with ultimate responsibility for mission accomplishment and resource management must have total authority for determining where and how OPSEC will be applied.

POLICY

A National Operations Security Program is hereby established. Each department and agency assigned or supporting national security missions with classified or sensitive activities shall establish a formal OPSEC program with the following common features:

- Specific assignment of responsibility for OPSEC direction and implementation.

- o Specific requirements to plan for and implement OPSEC in anticipation of and, where appropriate, during department or agency activity.

- o Direction to use OPSEC analytical techniques to assist in identifying vulnerabilities and to select appropriate OPSEC measures.

- o Institution of positive measures to ensure that all personnel, commensurate with their positions and security clearances, are aware of hostile intelligence threats and understand the OPSEC process.

- o Instructions to conduct an internal annual OPSEC review which will outline a department or agency's current OPSEC program and highlight successes or problem areas that may aid in other OPSEC programs.

- o Provisions for support of and cooperation with other departments and agencies in their OPSEC programs.

Agencies with minimal activities that could impact on national security need not establish a formal OPSEC program; however, they must cooperate with other departments and agencies to minimize damage to national security when OPSEC problems arise.

RESPONSIBILITIES

Heads of departments and agencies assigned or supporting national security missions. Establish organizational OPSEC programs; issue, as appropriate,

OPSEC policies, procedures, and planning guidance; and designate departmental and agency planners for OPSEC. Advise the NSC on OPSEC measures required of other departments and agencies in order to achieve and maintain effectiveness in operations or activities. JCS should advise the NSC of the impact of nonmilitary US policies on the effectiveness of OPSEC measures taken by the US military and recommend to the NSC policies that would minimize any adverse effects.

Chairman, Senior Interagency Group for Intelligence (SIG-I)

The SIG-I is designated as the NSC's instrumentality for national OPSEC policy formulation, resolution of conflicting interagency OPSEC issues, guidance on national level OPSEC training, technical OPSEC support, and advice to individual agencies. The National Operations Security Advisory Committee (NOAC), as part of the SIG-I structure and functioning under the aegis of the Interagency Group for Countermeasures (Policy) will:

- Provide the SIG-I structure with advice and recommendations concerning measures and methods for reducing OPSEC vulnerabilities and propose corrective measures.

- As requested, consult with and provide advice and recommendations to the various departments and agencies concerning OPSEC vulnerabilities and corrective measures.

- o On an ad hoc basis, chair forums for two or more agencies having competing interests or responsibilities with OPSEC implications that may affect national security interests. Analyze the issues and prepare advisory memoranda and recommendations for the competing agencies. In the event of an impasse, make appropriate recommendations to the SIG-I structure for resolution of the dispute.

- o Bring to the attention of the SIG-I those major unresolved OPSEC vulnerabilities and deficiencies that may arise within designated programs and activities of the executive branch.

- o Articulate to the SIG-I national-level requirements for intelligence and counterintelligence support to OPSEC.

Director, National Security Agency

The Director, National Security Agency, is designated Executive Agent for interagency OPSEC training and will assist departments and agencies, as needed, to establish their own OPSEC programs; develop and provide interagency OPSEC training courses; and establish and maintain an Interagency OPSEC Support Staff (IOSS), whose membership shall include, at a minimum, a representative of the Central Intelligence Agency, the Federal Bureau of Investigation, the General Services Administration, and the Departments of Defense and Energy. The IOSS will:

- Carry out interagency, national level, OPSEC training for executives, program and project managers, and OPSEC specialists.

- Act as consultant to individual departments and agencies for the establishment of OPSEC programs and for OPSEC surveys and analyses.

- Provide an OPSEC technical staff for the SIG-I.

Nothing in this Directive:

- Is intended to impinge on the authorities and responsibilities of the DCI to protect intelligence sources and methods, nor those of any authorized agency or department to conduct intelligence-related activities.

- Implies any authority on the part of the SIG-I, Interagency Group/Countermeasures (Policy), or the NOAC to examine the facilities or operations of any department or agency without the approval of the head of such department or agency.